REMARKS

Claims 4, 6-7 and 35-51 are pending. Claims 4, 7 and 39 are the independent claims.

I. Office Action Summary

In the final Office Action dated October 28, 2008, the Examiner rejected all of the claims as obvious over the combination of Hirota et al. (U.S. 6, 856,431 – "Hirota") and Dolan et al. (U.S. 5, 604,801 – "Dolan").

The Office Action, on page 2, also included a header reading: "***Election/Restrictions***", however no language relating to any election/restriction requirement follows that header. Applicant assumes that this header language was unintentional, but requests that the Examiner provide a new office action if any election/restriction was intended.

II. Rejections Under 35 U.S.C. § 103(a)

Applicants respectfully disagree with the Examiner's rejection the claims over Hirota et al. and Dolan et al.

CLAIM 4

Amended independent claim 4 recites a device for playback of encrypted audio and/or video tracks from a memory card. The device comprises:

> a processor; and
> a module operatively coupled with the processor and configured, for each audio and/or video file within an audio and/or video track, for:
> obtaining an encrypted key from a protected area of the memory card;
> retrieving only a portion of the audio and/or video file from the memory card;
> decrypting the obtained encrypted key;
> decrypting the portion of the audio and/or video file with the decrypted key; and

deleting the decrypted key after decrypting the portion of the audio and/or video file before decrypting an additional portion of the file.

Claim 4 has been amended to clarify an aspect that the cited art is lacking. Claim 4 recites a module that is configured for each audio and/or video file comprising an audio and/or video track to retrieve only a portion of the audio and/or video file, decrypt the portion of the file and delete the decrypted key before decrypting an additional portion of the file of the track.

Hirota fails to teach or suggest deleting a key as claimed. Hirota teaches a playback apparatus that plays tracks of audio made up of one or more encrypted files referred to as audio object (AOB) files. Each AOB file has a unique filename and has a "File Key" for decrypting the respective AOB file that has a name that substantially matches the name of the AOB file (Col. 10, lines 18-30; FIG. 9, Col. 13, lines 22-57). When an encrypted AOB file in Hirota is played back, the appropriate FileKey is retrieved and placed in RAM in a FileKey Storing Area 14 and the FileKey and is sent to descrambler 7 (FIG. 52; Col. 43, lines 1-6; Col. 44, lines 37-48). The FileKey is maintained in the descrambler while the entire AOB file is decrypted and played back (See Col. 47, lines 21-27). Hirota is completely missing at least the element of a module configured for "deleting the decrypted key after decrypting the portion of the audio and/or video file before decrypting an additional portion of the file".

Thus rather than teaching or suggesting the device of claim 4, where only a portion of the file is retrieved, a key is decrypted, the retrieved portion is decrypted with the decrypted key and then the key is deleted before decrypting another portion of the file, Hirota keeps the key in a descrambler until the file is decrypted. Claim 4 in its present form defines tracks having one or more files and a device for playback having a module configured for deleting a decrypted key after decrypting a portion of the file. As noted in the present disclosure, an advantage of only decrypting only a portion of a file and deleting the key each time a portion has been decrypted before going on to decrypt another portion is

that the amount of decrypted file is kept small and the key is only in a decrypted state for a very short time. In contrast Hirota discusses how it attempts to minimize the damage that exposing a FileKey will cause by using a separate FileKey for each AOB file, rather than a portion of a file, but that the key is left in the descrambler for the entire time a file is being decrypted.

Dolan is cited by the Examiner as allegedly disclosing the step of deleting the decrypted key before decrypting an additional portion of the file that is missing from Hirota. Applicant respectfully disagrees. Dolan discloses a communication system that uses a server, separate from a party sending a message, to perform public key processing on the message sent by a sending party, so that the sending party doesn't have to perform the public key processing on the sending party's portable security device (Col. 2, lines 54-64). The process disclosed in Dolan involves the message sending party sending a key encrypting key (KEYa), along with the message to be processed, to the server (FIG. 4a). The server then signs the message by decrypting a secret key (SKa) already stored on the server, signing the entire message using the secret key, and either forwarding the message or returning it to the sending party to send on to the recipient (Col. 6, line 66 – Col. 7, line 11; FIG. 4b). The decrypted secret key at the server is temporarily stored, used to digitally sign the message from the sending party, and then erased (Col. 7, lines 2-11; FIG. 4b).

Dolan fails to teach or suggest any of the elements of claim 4, including the step the Office Action admits is missing from Hirota. Claim 4 recites "deleting the decrypted key . . . before decrypting an additional portion." Dolan is related to a way of digitally signing communications in a communication system using standard public-private key encryption. Dolan is not related to a decryption process of items in a memory device. Dolan describes a form of outsourced ***encryption*** of ***entire*** messages in a communication system rather than decryption of portions of the content of an encrypted file in a memory. Dolan is unrelated to memory devices, discusses encryption (digitally signing) of

messages rather than decryption of data and discusses encryption for entire messages before deleting a key used to encrypt the message.

The final Office Action, on page 7, cites to the abstract and to column 4, lines 50-58 of Dolan. These cited sections merely note that keys used to encrypt a message are deleted after use. These cited sections, and the remainder of Dolan, do not recite decrypting portions of a file of a track retrieved from memory and deleting keys after each portion of the file of the track is decrypted. The keys in Dolan are used to encrypt entire messages and are deleted afterwards – Dolan does not teach or suggest deleting keys before an entire message has been encrypted, let alone the process of decrypting portions of files retrieved from memory and deleting keys after each portion of a file is decrypted.

Accordingly, Applicants respectfully submit that claim 4 distinguishes over Dolan and Hirota, alone or in combination for at least the above reasons. Claims 6 and 35-38 are dependent claims, therefore their allowability directly follows from the allowability of independent claim 4.

CLAIM 7

Claim 7 relates to a computer readable storage medium having an executable program configured to, for each encrypted audio or video file comprising an encrypted track:

> decrypt an encrypted audio or video file from the memory card,
>
> wherein decrypting the audio or video file comprises:
>
> (a) decrypting a key stored in the memory of the device;
>
> (b) decrypting a portion of the audio or video file less than an entirety of the audio or video file;
>
> (c) deleting the decrypted key; and
>
> (d) repeating (a) through (c) until the entirety of the audio or video file is decrypted.

Although of different scope than claim 4, claim 7 also recites the feature of deleting a decrypted key after each portion of a file is decrypted. Claim 7 has also been amended to clarify that the decrypted key is deleted after each portion of an encrypted file in a track is decrypted. Again, this is different than the teachings or suggestions found in Hirota, where a decrypted key is left in a descrambler for the decryption of an entire file, or Dolan, only discloses deleting a key after encrypting an entire message.

Accordingly, for at least these reasons, Applicants submit that claim 7 is allowable over the cited art.

CLAIM 39

Claim 39 recites a method for playback of audio and/or video tracks comprising one or more encrypted audio and/or video files stored on a memory, where the method includes:

> obtaining an encrypted key from a protected area of the memory card with a device having a processor and a memory operatively connected with the processor;
> retrieving only a portion of an audio and/or video file from the memory card with the device, wherein the audio and/or video file comprises at least a portion of an audio and/or video track;
> decrypting the encrypted key;
> decrypting the portion of the audio and/or video file with the decrypted key; and
> deleting the decrypted key from the device after decrypting the portion of the audio and/or video file before decrypting an additional portion of the audio and/or video file.

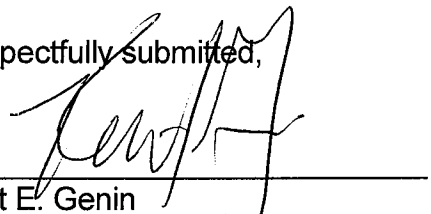
Although of different scope than claims 4 and 7, claim 39 recites steps relating to deleting a decrypted key after each portion of a track is decrypted and before the next portion of the file is decrypted. Accordingly for at least the same reasons as noted for claims 4 and 7, Applicants submit that claim 39 is allowable over the

cited art. Claims 40-51 are dependent claims. Accordingly, their allowability directly follows from the allowability of independent claim 39.

III. Conclusion

Applicants amended claims 4, 7, 36-37, 39-40, 42, 45-46 and 51. The amendments are fully supported by the specification and add no new matter. With the above remarks, Applicants submit that claims 4, 6-7 and 35-51 are in condition for allowance. A Notice of Allowance is respectfully requested.

Respectfully submitted,



BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

Kent E. Genin
Registration No. 37,834
Attorney for Applicants